IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): B.M. Jakobsson
Docket No.: 30-6
Serial No.: 09/712,335
Filing Date: November 14, 2000
Group: 2132
Examiner: Grigory Gurshman

Title: Software Aging Method and Apparatus for Discouraging Software Piracy

---

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Sir:

Applicants (hereinafter referred to as "Appellants") hereby appeal the final rejection of claims 1-15 in the above-referenced application.

REAL PARTY IN INTEREST

The present application is assigned to Lucent Technologies Inc. The assignee Lucent Technologies Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences.

STATUS OF CLAIMS

Claims 1-15 are pending in the application and stand rejected under 35 U.S.C. §103(a). The §103(a) rejection of claims 1-15 is appealed.

STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention as claimed includes a method, apparatus and machine-readable medium for discouraging unauthorized use of a software program, thereby facilitating the prevention of software piracy.

Independent claim 1 is directed to a method of discouraging unauthorized use of a software program. The method includes the step of configuring the software program in accordance with a software aging process such that one or more files generated by the program are at least partially encrypted using a first cryptographic key associated with a current time interval for which the files are generated. The method further includes the step of providing periodic updates of the software program to a legitimate user of the software program, with a given one of the periodic updates including at least a second cryptographic key associated with a time interval subsequent to the current time interval.

A flow diagram of an illustrative embodiment of the invention is shown in FIG. 4, and described in the specification at page 11, line 18, to page 12, line 21. This embodiment discourages software piracy by essentially forcing all users to perform frequent automatic updates. More specifically, as indicated in step 42, user software encrypts at least a portion of each file it generates, using a symmetric key that is common to all copies of that version of the software. Thus, the utility of a prior version held by an illegitimate user will continually degrade over time since it will be unable to read files generated using the current and later versions.

Independent claim 14 is an apparatus version of independent claim 1, and comprises processor and memory elements, examples of which can be seen as respective elements 20 and 22 of FIG. 2.

Independent claim 15 is directed to a machine-readable medium which contains a software program which is configured and periodically updated in a manner similar to that recited in independent claim 1.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-15 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,870,468 to Harrison (hereinafter "Harrison") in view of U.S. Patent No. 5,784,464 to Akiyama (hereinafter "Akiyama").

ARGUMENT

Appellants incorporate by reference herein the disclosures of all previous responses filed in the present application, namely, responses dated December 8, 2004 and May 19, 2005.

Claims 1, 3, 4 and 11-15

Appellants initially note that a proper *prima facie* case of obviousness requires that the cited references, when combined, must "teach or suggest all the claim limitations," and that "there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings." See MPEP §706.02(j).

Independent claims 1, 14 and 15 each describe the encrypting of one or more files "using a first cryptographic key associated with a current time interval for which the files are generated." In formulating the §103(a) rejection, the Examiner argues that this element of the claims is taught by Harrison. More specifically the Examiner states as follows at page 4, section 10, of the Final Office Action:

> Referring to the independent claims 1, 14 and 15, the limitation "configuring the software program . . . such that one or more files generated by the program are ate (*sic*) least partially encrypted using a first cryptographic (*sic*) associated with a current time interval . . ." is met by file protection agent software (18) depicted in Fig. 2, which encrypts files with encryption key. The key is generated for the particular set of files (see Fig. 1) and the key

> is used in accordance with the preset time limit (see block 6). Therefore the encryption key is associated with the time interval, as recited in the instant claims.

Appellants respectfully disagree. One skilled in the art will immediately recognize that Harrison teaches "a time interval" element that is entirely different in nature from that recited in the independent claims of the present invention. The time interval described by Harrison (block 6 of FIG. 1) is a user-defined "File Unprotected Time interval" which "will determine how long a file in the File Protection List . . . may remain unencrypted (or unprotected) after being closed" (Harrison, col. 3, lines 9-12, *emphasis added*). After this time period runs, an unencrypted file is automatically encrypted (see Harrison, col. 3, line 59 to col. 4, line 9; and FIG. 5, element 16). Harrison's time interval is, therefore, merely a time limit, and is referred to as such in Harrison's FIG. 1, elements 6 and 7. Claims 1, 14 and 15, on the other hand, describe an entirely different type of time interval. The time interval in these claims is the "current time interval for which the files are generated." Accordingly, this time interval unambiguously describes the period of time in which the files are encrypted. Notably, it is the variation in the cryptographic key from one such time period to another in accordance with the invention that acts to enable the invention to discourage the unauthorized use of software. See, for example, Specification at p. 3, lines 11-17.

Appellants respectfully submit, therefore, that Harrison teaches an encryption process with a user-defined time limit on the encryption state of any given file rather than an encryption key associated with a current time interval like that described in claims 1, 14 and 15. Moreover, Akiyama fails to remedy this fundamental deficiency in Harrison as applied to the independent claims. As a result, it is believed that claims 1, 14 and 15 would not have been obvious at the time of the invention over Harrison in view of Akiyama.

It is further noted that, with respect to providing a motivation for combining Harrison and Akiyama, the Examiner argues the following at page 5, section 10, of the Final Office Action:

> One of ordinary skill in the art would have been motivated to have a software program configured to encrypt files with the key associated with the time interval and provide periodic updates including encryption keys associated with subsequent time intervals as taught in Akiyama for eliminating a risk of the unlawful decryption thereof by a third party (see Akiyama column 17, lines 66-68).

The Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination "must be based on objective evidence of record" and that "this precedent has been reinforced in myriad decisions, and cannot be dispensed with." In re Sang-Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Moreover, the Federal Circuit has stated that "conclusory statements" by an examiner fail to adequately address the factual questions of motivation, which is material to patentability and cannot be resolved "on subjective belief and unknown authority."Id. at 1343-1344. Appellants respectfully submit that this §103(a) rejection contains no such showing of objective evidence of record that would motivate one skilled in the art to combine the proposed references. Without characterizing Akiyama, Appellants submit that, absent the use of improper hindsight, periodically changing encryption keys to eliminate unlawful decryption by unauthorized third parties does not motivate one skilled in the art to modify Harrison in a way which meets the particular limitations of the independent claims.

Dependent claims 3, 4 and 11-13 are believed to be allowable over Harrison in view of Akiyama for at least the reasons stated above with regard to independent claim 1.

Claim 2

Appellants assert that claim 2 is allowable for at least the reasons stated above with respect to independent claim 1.

Appellants also assert that claim 2 contains separately-patentable subject matter. Claim 2 specifies that at least a subset of the periodic updates do not provide any alteration of the functionality of the program but instead discourage piracy of the program through alteration of the cryptographic key used to at least partially encrypt outputs generated by the program. The Examiner argues that these limitations are met by the arrangement shown in FIG. 6 of Harrison. See the Final Office Action at page 5, section 11. However, it appears that the Examiner fails to address the particular limitations of the claim. Also, Appellants have been unable to locate any teaching or suggestion regarding the limitations at issue in the relied-upon figure or its associated textual description.

Accordingly, it is believed that the proposed combination of Harrison and Akiyama fails to meet the limitations of claim 2.

Claim 5

Appellants assert that claim 5 is allowable for at least the reasons stated above with respect to independent claim 1.

Appellants also assert that claim 5 contains separately-patentable subject matter. Claim 5 specifies that the first cryptographic key is computable as a function of the second cryptographic key using a publicly-known one-way function. The Examiner relies on column 17 of Akiyama. See the Final Office Action at page 5, section 13. Appellants have reviewed the relied-upon portion of Akiyama, and are unable to locate therein any teaching or suggestion regarding a key relationship via one-way function as recited in claim 5.

Accordingly, it is believed that the proposed combination of Harrison and Akiyama fails to meet the limitations of claim 5.

Claim 6

Appellants assert that claim 6 is allowable for at least the reasons stated above with respect to independent claim 1.

Appellants also assert that claim 6 contains separately-patentable subject matter. Claim 6 specifies that each file generated by the software program in a given time interval is labeled with an identifier of the time interval. The Examiner apparently fails to address these particular limitations in the Final Office Action. Appellants therefore respectfully submit that this rejection does not meet the specificity requirements under the Federal Regulations and the MPEP. 37 C.F.R. §1.104(c)(2) requires:

> In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified. (*emphasis added*)

Moreover, MPEP §706 requires that "[w]hen a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated

as nearly as practicable." The rejection of claim 6 is therefore deficient with respect to these requirements. Moreover, Appellants have been unable to locate the recited limitations in the relied-upon references.

Accordingly, it is believed that the proposed combination of Harrison and Akiyama fails to meet the limitations of claim 6.

Claim 7

Appellants assert that claim 7 is allowable for at least the reasons stated above with respect to independent claim 1.

Appellants also assert that claim 7 contains separately-patentable subject matter. Claim 7 specifies that the time interval identifier uniquely identifies a particular cryptographic key that may be used to decrypt an encrypted portion of a file for that interval. The Examiner relies on FIG. 5 of Harrison and the association of timer 33 with encryption key 3. See the Office Action at page 5, section 14. Appellants respectfully disagree. The relied-upon portion of Harrison simply fails to teach or suggest a time interval identifier which uniquely identifies a particular cryptographic key as recited.

Accordingly, it is believed that the proposed combination of Harrison and Akiyama fails to meet the limitations of claim 7.

Claim 8

Appellants assert that claim 8 is allowable for at least the reasons stated above with respect to independent claim 1.

Appellants also assert that claim 8 contains separately-patentable subject matter. Claim 8 specifies that the first encryption key is common to each of a plurality of legitimate copies of the software program that have received a corresponding version of the update. The Examiner provides no specific arguments as to why this claim is unpatentable over Harrison in view of Akiyama beyond that provided for independent claim 1. The rejection of claim 8 is therefore improper. See 37 C.F.R. §1.104(c)(2); MPEP §706. Moreover, Appellants have been unable to locate the recited limitations in the relied-upon references.

Accordingly, it is believed that the proposed combination of Harrison and Akiyama fails to meet the limitations of claim 8.

Claim 9

Appellants assert that claim 9 is allowable for at least the reasons stated above with respect to independent claim 1.

Appellants also assert that claim 9 contains separately-patentable subject matter. Claim 9 recites the step of providing periodic random updates of the software program to one or more illegitimate users, a given one of the random updates including a random number in place of an cryptographic key associated with a correct update. The Examiner provides no specific arguments as to why this claim is unpatentable over Harrison in view of Akiyama beyond that provided for independent claim 1. The rejection of claim 9 is therefore improper. See 37 C.F.R. § 1.104(c)(2); MPEP §706. Moreover, Appellants have been unable to locate the recited limitations in the relied-upon references.

Accordingly, it is believed that the proposed combination of Harrison and Akiyama fails to meet the limitations of claim 9.

Claim 10

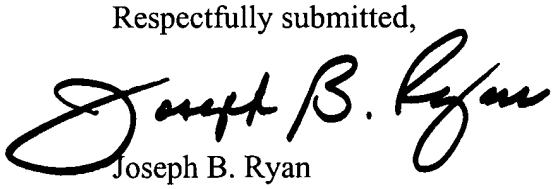
Appellants assert that claim 10 is allowable for at least the reasons stated above with respect to independent claim 1.

Appellants also assert that claim 10 contains separately-patentable subject matter. Claim 10 specifies that files generated by the software program for a current time interval t using the first cryptographic key are readable only by copies of the program that have received an update corresponding to at least an interval t-δ, where δ is a designated number of time intervals for which compatibility between current and previous versions is desired. The Examiner again relies on FIG. 6 of Harrison, but Appellants are unable to find the recited limitations in this figure or its associated textual description.

Accordingly, it is believed that the proposed combination of Harrison and Akiyama fails to meet the limitations of claim 10.

For at least the reasons given above, Appellants respectfully request withdrawal of the §103(a) rejection of claims 1-15.

Respectfully submitted,



Date: August 23, 2005

Joseph B. Ryan
Attorney for Appellant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

CLAIMS APPENDIX

1. A method of discouraging unauthorized use of a software program, the method comprising the steps of:

configuring the software program in accordance with a software aging process such that one or more files generated by the program are at least partially encrypted using a first cryptographic key associated with a current time interval for which the files are generated; and

providing periodic updates of the software program to a legitimate user of the software program, a given one of the periodic updates including at least a second cryptographic key associated with a time interval subsequent to the current time interval.

2. The method of claim 1 wherein at least a subset of the periodic updates do not provide any alteration of the functionality of the program but instead discourage piracy of the program through alteration of the cryptographic key used to at least partially encrypt outputs generated by the program.

3. The method of claim 1 wherein the files generated by the program for the current time interval and at least partially encrypted using the first cryptographic key are readable only by programs having a corresponding decryption key.

4. The method of claim 3 wherein the first cryptographic key and the corresponding decryption key comprise a common symmetric cryptographic key used for both encryption and decryption.

5. The method of claim 1 wherein the first cryptographic key is computable as a function of the second cryptographic key using a publicly-known one-way function.

6. The method of claim 1 wherein each file generated by the software program in a given time interval is labeled with an identifier of the time interval.

7. The method of claim 6 wherein the time interval identifier uniquely identifies a particular cryptographic key that may be used to decrypt an encrypted portion of a file for that interval.

8. The method of claim 1 wherein the first encryption key is common to each of a plurality of legitimate copies of the software program that have received a corresponding version of the update.

9. The method of claim 1 further including the step of providing periodic random updates of the software program to one or more illegitimate users, a given one of the random updates including a random number in place of an cryptographic key associated with a correct update.

10. The method of claim 1 wherein files generated by the software program for a current time interval t using the first cryptographic key are readable only by copies of the program that have received an update corresponding to at least an interval t-δ, where δ is a designated number of time intervals for which compatibility between current and previous versions is desired.

11. The method of claim 1 wherein at least a subset of the periodic updates are provided to the legitimate user over a network connection established with a distributor of the software program.

12. The method of claim 1 wherein at least a subset of the periodic updates are provided to the legitimate user in an automatic manner so as not to be apparent to an operator of the software program.

13. The method of claim 1 wherein the legitimate user is identified as such by a distributor through the use of an identifier associated with one of a number of known legitimate copies of the software program.

14. An apparatus for discouraging unauthorized use of a software program, the apparatus comprising:

a memory for storing at least a portion of the software program; and

a processor coupled to the memory and operative to execute at least a portion of the software program, wherein the software program is configured in accordance with a software aging process such that one or more files generated by the program are at least partially encrypted using a first cryptographic key associated with a current time interval for which the files are generated;

wherein periodic updates of the software program are provided to a legitimate user of the software program, a given one of the periodic updates including at least a second cryptographic key associated with a time interval subsequent to the current time interval.

15. A machine-readable medium containing a software program, executable on a digital data processor comprising a processor and a memory, configured in accordance with a software aging process such that one or more files generated by the program are at least partially encrypted using a first cryptographic key associated with a current time interval for which the files are generated, wherein periodic updates of the software program are provided to a legitimate user of the software program, a given one of the periodic updates including at least a second cryptographic key associated with a time interval subsequent to the current time interval, such that the variation of cryptographic keys from one of the intervals to another of the intervals discourages unauthorized use of the software program.

EVIDENCE APPENDIX

(None)

RELATED PROCEEDINGS APPENDIX

(None)